Complaint IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JOHNNY FLORES, ARIEL GOMEZ and DERRICK LEWIS, for themselves and others similarly situated, Plaintiff, v. MOTOROLA SOLUTIONS, INC., and VIGILANT SOLUTIONS, LLC, Defendants.	)	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED** **INJUNCTIVE RELIEF DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Johnny Flores, Ariel Gomez and Derrick Lewis, by and through their attorneys Loevy & Loevy, brings this Class Action Complaint against Defendants MOTOROLA SOLUTIONS, INC. ("MOTOROLA") and VIGILANT SOLUTIONS, LLC ("VIGILANT"), on behalf of themselves and all other similarly situated individuals ("Plaintiffs"), and as follows:

INTRODUCTION

1. Every individual has unique features by which he or she can be identified using a set of standard quantitative measurements. For example, the shape of and distance between tiny ridges on each person's finger are unique, so measures of these features—an example of "biometric" data—can be used to identify a specific individual as the person who made a fingerprint. Similarly, each person also has a unique facial geometry composed of, among other measures, distances between key facial landmarks and ratios between those distances. Once a picture of person's face is scanned and those biometric measurements are captured, computers

can store that information and use it to identify that individual any other time that person's face appears on the internet, in a scanned picture, and potentially in any of the billions of cameras that are constantly monitoring our daily lives. Unlike fingerprints, however, facial biometrics are readily observable and, thus, present an even graver and more immediate danger to privacy, individual autonomy, and liberty. This fact about human facial geometry, the technologies that record it, and the opportunities for surveillance those technologies enable present grave challenges to traditional notions of privacy that people have expected since time immemorial.

2. As the Illinois General Assembly has found: "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." 740 ILCS § 14/5(c).

3. Pursuant to Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS §14/1, *et seq.*, Illinois prohibits private entities from, among other things, collecting, capturing, obtaining, disclosing, redisclosing, disseminating or profiting from the biometric identifiers or information of an individual without providing written notice and without obtain a written release from the impacted individual or his authorized representative. BIPA also requires private entities in possession of biometric identifiers to adopt retention and destruction policies and to take measures to prevent the release of that information.

4. In violation of BIPA, Defendants Motorola and Vigilant collected, captured, obtained, disclosed, redisclosed, disseminated and profited from the facial geometric scans of hundreds of thousands of Illinois citizens in violation of BIPA's requirements. Specifically,

Vigilant, with Motorola later joining, collected and presently maintain a "gallery" of over 18 million booking photos or "mugshots" which is expanding all the time. The "gallery" includes at least tens of thousands of Illinois residents (many of whom were innocent and/or have had their records expunged by court order). Defendants have extracted the facial biometrics of each of person without permission.

5. In particular, Defendants performed a scan of the facial geometry of each depicted individual, stored the resultant biometric identifiers and information in a proprietary database (the "Biometric Database"), and disclosed, redisclosed, and otherwise disseminated those biometric identifiers and information to third parties in order to profit.

6. Defendants possess the biometric identifiers and information of the individuals in its Biometric Database without having adopted or made public any policy, written or otherwise, to govern the retention and destruction of thereof.

7. Defendants engaged in the above-described conduct: (a) without informing the impacted individuals that their biometric identifiers and information were being collected, captured, obtained, disclosed, redisclosed and otherwise disseminated; (b) without informing the impacted individuals in writing of the purpose of the collection, capture, obtainment, disclosure, redisclosure or dissemination of the biometric identifiers and information; and (c) without seeking or obtaining written releases from such impacted individuals or their authorized representatives.

8. In violation of BIPA, Defendants have also profited, and continues to profit, from their unlawful collection, possession, disclosure, and dissemination of the biometric identifiers and information of Plaintiffs and members of the proposed class (the "Class Members"). For a fee, Defendants offer law enforcement agencies and others throughout the country the

opportunity to access and use their Biometric Database as a "facial search engine" allowing the identification of persons in the database. Defendants also incorporate the Biometric Database into their other facial recognition products thereby allowing the identification and tracking in real time and near-real time of millions of people—including Plaintiff and Class Members—wherever they may go.

9. To be included in Defendants' Biometric Database, a person merely had to have been arrested. To Defendants, it did not and does not matter whether that arrest resulted in a conviction or had been made in error or whether the booking photo has been expunged. Thus, like the guests of the Hotel California, Plaintiffs and the Class Members can never leave, at least not until this Court grants the requested relief.

10. As the Illinois General Assembly has found and the Illinois Supreme Court has confirmed, the harm to Plaintiffs and Class Members has already occurred.

11. Public policy in Illinois provides that given the risks of unwanted data collection and disclosure, its citizens need the power to make decisions about the fate of their unique biometric identifiers and information.

12. As a direct result of Defendants' actions, Plaintiffs' and Class Members' biometric identifiers and information are no longer under their control and are now available to a potentially unlimited range of unknown individuals—both employees and clients of Defendants—who can surveil Plaintiffs and Class Members now and in the future. The injuries described herein are imminent and certainly impending.

13. Plaintiffs bring this Class Action Complaint seeking: (a) statutory damages of $5,000 per BIPA violation, or in the alternative, $1,000 per BIPA violation, from each of the Defendants, along with attorneys' fees and costs; (b) disgorgement of Defendants' ill-gotten

gains derived from the unlawful collection, possession, sale, disclosure, redisclosure, and dissemination of the unlawfully-acquired data; and (c) an injunction ordering that Defendants delete the data from its database.

PARTIES

14. Plaintiff Derrick Lewis is an Illinois resident. At times relevant to this case, Mr. Lewis was incarcerated at the Illinois Department of Corrections and at the Cook County Jail, including on charges of which he was innocent and convictions which have been vacated on the basis of innocence and expunged. Those entities made his and all detainees' booking photograph(s) searchable on their websites. On information and belief, Defendants are in possession of Mr. Lewis' booking photograph(s), have used it to extract his biometric identifiers and are currently in possession of his biometric identifiers and information.

15. Plaintiff Johnny Flores is an Illinois resident. At times relevant to this case, Mr. Flores was incarcerated at the Illinois Department of Corrections on a charge of which he was innocent. He was released in November of 2018 and is challenging his conviction in a post-conviction proceeding. A booking photograph of him remains on the Illinois Department of Corrections website to this day. On information and belief, Defendants are in possession of his booking photo(s), have used it to extract his biometric identifiers and are currently in possession of his biometric identifiers and information.

16. Plaintiff Ariel Gomez is an Illinois resident. At times relevant to this case, Mr. Gomez was incarcerated at the Illinois Department of Corrections on a charge of which he was innocent. After 20 years of incarceration for a crime he did not commit, his conviction was vacated and the charges against him dismissed. On information and belief, Defendants are in

possession of his booking photo(s), have used it to extract his biometric identifiers and are currently in possession of his biometric identifiers and information.

17. Plaintiffs seek to represent a class of current and former residents of Illinois whose pictures appear in Defendants' Biometric Database.

18. Defendant Vigilant Solutions LLC is a Delaware corporation wholly owned by Defendant Motorola. Motorola Solutions, Inc. is a Delaware Corporation with its principal place of business in Chicago, Illinois.

19. On or about January 2019, Defendant Vigilant became a part of Defendant Motorola. Much of the marketing takes place in and touts the companies' connection to each other and to Illinois. For example, Vigilant's LinkedIn banner states: "Now Part Of The Motorola Solutions Platform." The famous Motorola logo appears higher on Vigilant's Linkedin page than does its own obscure logo. The same is true of Vigilant's Twitter page which is not titled to the Vigilant company but: "Vigilant from Motorola Solutions." The company recently tweeted a photograph of the Chicago skyline, lakefront and Lake Shore Drive with the caption: "From Our Home To Yours, Wishing You a Happy Thanksgiving. Vigilant Solutions."

20. Vigilant and Motorola also recently marketed their facial recognition products at the 2019 International Association of Chiefs of Police (IACP) convention in McCormick Place stating: "Vigilant is now part of Motorola Solutions" with a picture of the skyline along the Chicago River. As another example of the companies' partnership and connection to Illinois, Motorola marketed a facial recognition "lunch and learn" on its twitter feed, held at the Westmont Police Department on February 6, 2020 and at the Rockford Police Department prior to that.

JURISDICTION AND VENUE

21. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) (the "Class Action Fairness Act") because sufficient diversity of citizenship exists between the parties in this action, the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, and there are 100 or more members of the Class. Because it is estimated that the Class will have tens of thousands of members and Defendants' intentional and reckless violations of BIPA are punishable by statutory damages of $5,000 per violation, the amount in controversy is well in excess of $5,000,000. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

22. This Court has personal jurisdiction over Defendant Vigilant because it collected, or participated in collecting, and currently maintains the booking photos taken of Plaintiffs and Class Members in Illinois. Defendant knew that its collection, capture, obtainment, disclosure, redisclosure and dissemination of impacted individuals' biometric identifiers and information would injure Illinois residents. Those unlawful acts, committed in violation of the rights of Illinois residents using the resources of Illinois jurisdictions, are at the center of this suit. Vigilant is also conducts its marketing from and within Illinois as well as in a partnership with Motorola, which is a resident of Illinois. Vigilant also profits by contracting with law enforcement agencies throughout Illinois, including those in Chicago, Burr Ridge, and Rockford, to provide access to its surveillance technology. Vigilant knew or had reason to know that collecting, capturing, obtaining, disclosing, redisclosing and disseminating Illinois citizens' and residents' biometric identifiers and information without providing the requisite consent and obtaining the requisite releases would deprive Illinois citizens and residents of their statutorily-protected privacy rights, neutralize Illinois citizens' and residents' ability to control access to

their biometric identifiers and information, and expose Illinois citizens and residents to potential surveillance and other privacy harms.

23. This Court has personal jurisdiction of Defendant Motorola, because it has its principal place of business in Chicago, Illinois.

24. Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the acts or omissions giving rise to the claim occurred in Illinois. Alternatively, venue is proper under 28 U.S.C. § 1391(b)(3) because this Court has personal jurisdiction over Defendants Vigilant and/or Motorola.

ILLINIOIS BIOMETRIC PRIVACY LAWS

25. BIPA seeks to safeguard individuals' biometric identifiers and information.

26. Biometric identifiers include a scan of an individual's face geometry. 740 ILCS § 14/10.

27. Biometric information is "any information . . . based on an individual's biometric identifier used to identify an individual." 740 ILCS § 14/10.

28. Pursuant to BIPA, a private entity, such as Defendants, are among other things: (a) prohibited from collecting, capturing or otherwise obtaining an individual's biometric identifiers and information without providing written notice and obtaining a written release; (b) prohibited from selling, leasing, trading or otherwise profiting from an individual's biometric identifiers and information; (c) prohibited from disclosing, redisclosing or otherwise disseminating an individual's biometric identifiers or information in the absence of circumstances specifically set forth in the statute; and (d) required, to the extent it is in possession of biometric identifiers or information, to develop a written policy, made available to

the public, that establishes a retention schedule and guidelines for permanently destroying such identifiers and information. 740 ILCS § 14/15.

29. BIPA provides for a private right of action and allows a prevailing party to recover liquidated damages in the amount of: (a) $1,000 or actual damages, whichever is greater, for negligent violations of its provisions; and (b) $5,000 or actual damages, whichever is greater, for intentional or reckless violations of its provisions. 740 ILCS § 14/20. BIPA also allows for the recovery of attorneys' fees and costs and injunctive relief. 740 ILCS § 14/20.

ALLEGATIONS

I. Allegations Related to Named Plaintiffs

30. Defendants populate the Biometric Database with over 18 million booking photographs, constantly updating it with new photos as they appear. Among these are the booking photographs that are appear and are searchable on the Illinois Department of Corrections ("IDOC") inmate search websites. Defendant Vigilant began obtaining the booking photographs it uses no later than 2014. On information and belief, the Biometric Database includes Plaintiffs' booking photographs because, among other reasons, they were each at IDOC after Vigilant began collecting the booking photos and their photos were available on the website.

31. For each of their photographs, Defendants, singularly and/or in concert, scanned their facial geometry; and included their photos, biometric information, and other identifying information – including, *inter alia*, their names and other information in the Biometric Database.

32. After surreptitiously obtaining Plaintiffs' biometric identifiers and information, Defendants, singularly and/or in concert, disclosed, redisclosed, disseminated, sold, traded, and profited from Plaintiffs' biometric identifiers and information.

33. To this day, Defendants have (a) failed and continue to fail to advise Plaintiffs that they were performing scans of their facial geometries; (b) failed and continue to fail to inform Plaintiffs in writing or otherwise of the purpose for which it was collecting, capturing, obtaining, disclosing, redisclosing and disseminating Plaintiffs' biometric identifiers and information; (c) failed and continue to fail to adopt a policy about and to make publically available notice about the length of time they would retain Plaintiffs' identifiers and information and guidelines for how they would destroy it; (d) failed and continue to fail to permanently destroy Plaintiffs' identifiers after the initial purpose for collecting or obtaining such identifiers or information has been satisfied and/or within 3 years of the individual's last interaction with the private entity (which there never was) and (e) never sought, nor received, a written release from Plaintiffs or their authorized representatives that allowed them to collect, capture, obtain, disclose, redisclose and disseminate Plaintiffs' biometric identifiers and information.

34. Defendants' conduct has injured Plaintiffs or, alternatively, the injury to Plaintiffs is imminent and certainly impending.

II. Defendants' Unlawful Conduct

35. Defendants sell a range of surveillance and facial recognition products to government agencies and private companies throughout the United States, including the Motorola Command Center Software Suite, "FaceSearch" technology, license plate readers, video "Lineups" of real time or near-real time public video, Avigilon, and others.

36. According to Defendant Vigilant, the "facial recognition technology utilizes biometric algorithms of facial landmarks to find potential matches to help law enforcement develop strong investigative leads."

37. When Defendants acquire a mugshot or booking photo, they scan the facial geometry of the individual in the photo so that the resulting biometric identifiers and information can be matched against future unknown individuals.

38. When one of Defendant's customers uploads a "probe image" to the facial recognition application, the "algorithm creates a face print of the probe image." and "[f]acial recognition compares the probe image against the image gallery."

39. As of 2019, Defendants claimed that the Biometric Database provided access to 18 million open-source images, including the "mugshots," against which the "probe images" are compared.

40. At relevant times, the Biometric Database included IDOC booking photos and, on information and belief, publicly-available booking photos from other Illinois correctional and law enforcement agencies.

41. On information and belief, Defendants: (a) acquired Plaintiffs' and Class Members' booking photos; (b) collected, captured and otherwise obtained Plaintiffs' and Class Members' biometric identifiers and information from those images; and (c) disclosed, redisclosed, disseminated, sold, and otherwise profited from those biometric identifiers and information.

42. Defendants engaged in the above-described conduct without complying with BIPA's notice or consent provisions.

43. In collecting, capturing and otherwise obtaining the biometric identifiers and information of Plaintiffs and Class Members and, subsequently, disclosing, redisclosing and otherwise disseminating those biometric identifiers and information – all without providing the

requisite notice, obtaining the requisite releases or satisfying any of BIPA's other provisions that would excuse it from BIPA's mandates – Defendants again violated BIPA.

44. In further violation of BIPA, Defendants failed to use a reasonable standard of care to protect Plaintiffs' and Class Members' biometric identifiers and information from disclosure and, in fact, affirmatively disclosed Plaintiffs' and Class Members' identifiers and information.

45. In further violation of BIPA, as a private entity in possession of Plaintiffs' and Class Members' biometric identifiers and information, Defendants have failed to adopt or make available to the public a retention schedule or guidelines for permanently destroying such biometric identifiers and information once the initial purpose for collecting them has been satisfied.

46. In further violation of BIPA, Defendants also sold, leased, traded, and otherwise profited from the biometric identifiers and information of Plaintiffs and Class Members.

47. In further violation of BIPA, Defendants also failed and continue to fail to permanently destroy Plaintiffs' and the Class Members' identifiers after the initial purpose for collecting or obtaining such identifiers or information has been satisfied and/or within 3 years of the individual's last interaction with the private entity (which there never was).

48. In sum, whether selling FaceSearch or products incorporating the technology Defendants did exactly what BIPA prohibits.

49. Defendants' violations of BIPA were intentional and reckless or, in the alternative, negligent.

III. Plaintiffs' and Class Members' Injuries and Damages

50. As a result of Defendants' unlawful conduct, Plaintiffs and Class Members have already sustained injuries and face many more imminent and certainly impending injuries, which injuries they will continue to suffer.

51. Defendants' unlawful conduct has resulted in, among other things: (a) Plaintiffs' and Class Members' unique biometric identifiers and information being collected, captured, obtained, disclosed, redisclosed, and otherwise disseminated without the requisite notice having been given and without the requisite releases having been obtained; (b) Plaintiffs and Class Members being deprived of the very control over their biometric identifiers and information that BIPA was designed to protect; and (c) Plaintiffs and the Class Members being left without any understanding or security of when and how their biometric information and identifiers would finally be destroyed. .

52. Further, as a result of Defendants' unlawful conduct, Plaintiffs and Class Members do not know which, or how many, individuals or entities have received, obtained, accessed, stored, disclosed, redisclosed or otherwise made use of their biometric identifiers and information, exposing them to the imminent and certainly impending injuries of surveillance, reputational harm, stalking, and other privacy harms.[1]

53. Plaintiffs and Class Members have no recourse for the fact that Defendants compromised their unique biometric identifiers and information. Moreover, Plaintiffs and Class Members are at heightened risk for other potential injuries and are likely to withdraw from biometric-facilitated transactions and other facially-mediated electronic participation.

[1] *Facial Recognition Tech: 10 Views on Risks and Rewards*, https://www.forbes.com/sites/forbestechcouncil/2018/04/03/facial-recognition-tech-10-views-on-risks-and-rewards/#54d3e1716b3c (accessed on Feb. 1, 2020)

CLASS ACTION ALLEGATIONS

54. Plaintiff brings this action on behalf of themselves and similarly situated individuals as a class action under Federal Rule of Civil Procedure 23, seeking damages and equitable relief on behalf of the following Class for which Plaintiff seeks certification: All Illinois residents whose faces appeared in the Biometric Database during the period February 14, 2015 to the present.

55. Excluded from the Class are: (a) Defendants Vigilant and Motorola; (b) any of their parents, affiliates or subsidiaries; (c) any entities in which Defendants have a controlling interest; (d) any of Defendants' officers or directors; or (e) any successors or assigns of Defendants. Also excluded are any judge or court personnel assigned to this case and members of their immediate families.

56. Plaintiff reserves the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

57. **Numerosity.** While the exact number of Class members is not known at this time, Defendants collected, captured, obtained, disclosed, redisclosed, otherwise disseminated, sold, leased, traded, profited from and currently maintain the biometric identifiers and information from at least 18 million images of faces, of which, on information and belief, hundreds of thousands are photos of Illinois residents. The Class, therefore, likely includes tens of thousands of unique individuals. Consistent with Rule 23(a)(1), the proposed Class is therefore so numerous that joinder of all members is impracticable. Class Members may be identified through objective means, including objective data available to Defendants regarding the images in the Biometric Database and associated names and residency information. Class Members may be notified of the pendency of this action by recognized, Court-approved notice

dissemination methods, which may include U.S. mail, electronic mail, internet postings, social media and/or published notice.

58. **Commonality and predominance.** Common questions of law and fact exist as to all Class Members. These common questions of law or fact predominate over any questions affecting only individual members of the proposed Class. Common questions include, but are not limited to, the following:

a. Whether Defendants collected, captured, otherwise obtained and/or currently maintain the biometric identifiers or information of Plaintiffs and Class Members;

b. Whether Defendants possess or possessed the biometric identifiers or information of Plaintiffs and Class Members;

c. Whether Defendants disclosed, redisclosed or otherwise disseminated the biometric identifiers or information of Plaintiffs and Class Members;

d. Whether Defendants sold, leased, traded or otherwise profited from the biometric identifiers or information of Plaintiffs and Class Members;

e. Whether Defendants provided the notice required by BIPA before collecting, capturing, obtaining, disclosing, redisclosing or otherwise disseminating the biometric identifiers or information of Plaintiffs and Class Members;

f. Whether Defendants obtained written releases from Plaintiffs and Class Members or their authorized representatives before collecting, capturing, obtaining, disclosing, redisclosing or otherwise disseminating the biometric identifiers and information or Plaintiffs and Class Members;

g. Whether Defendants had in place – and disclosed to the public – the written retention and destruction policies required by BIPA while in possession of Plaintiffs' and Class Members' biometric identifiers and information;

h. Whether Plaintiffs and Class Members suffered damages as a proximate result of Defendants conduct;

i. Whether Defendants protected Plaintiffs' and Class Members' biometric identifiers and information from disclosure using the reasonable standard of care within the industry and in a manner that was the same as or more protective than the manner in which each of them protects other confidential and sensitive information; and

j. Whether Plaintiffs and Class Members are entitled to damages, equitable relief and other relief.

59. **Typicality.** Plaintiffs' claims are typical of the claims of the Class they seek to represent because Plaintiffs and all members of the proposed Class have suffered similar injuries as a result of the same practices alleged herein. Plaintiffs have no interests to advance adverse to the interests of the other members of the proposed Class.

60. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the proposed Class and have retained as his counsel attorneys experienced in class actions and complex litigation.

61. **Superiority.** A class action is superior to other available means for the fair and efficient adjudication of this dispute. The injury suffered by each Class Member, while meaningful on an individual basis, may not be of such magnitude as to make the prosecution of

individual actions against Defendants economically feasible. Even if Class Members could afford individual litigation, those actions would put immeasurable strain on the court system. Moreover, individual litigation of the legal and factual issues of the case would increase the delay and expense to all parties and the court system. A class action, however, presents far fewer management difficulties and provides the benefit of a single adjudication, economy of scale and comprehensive supervision by a single court.

62. In the alternative, the proposed Class may be certified because:

a. The prosecution of separate actions by each individual member of the proposed Class would create a risk of inconsistent adjudications, which could establish incompatible standards of conduct for Defendants;

b. The prosecution of individual actions could result in adjudications that as a practical matter would be dispositive of the interests of non-party Class Members or which would substantially impair their ability to protect their interests; and

c. Defendants acted or refused to act on grounds generally applicable to the proposed Class, thereby making final and injunctive relief appropriate with respect to members of the proposed Class.

63. Pursuant to Rule 23(c)(4), particular issues are appropriate for certification – namely the issues described above – because resolution of such issues would advance the disposition of the matter and the parties' interests therein.

CLAIMS FOR RELIEF

COUNT ONE
(VIOLATION OF BIPA – 740 ILCS § 14/15(a))

64. Plaintiffs restate and reallege all paragraphs of this Class Action Complaint as though fully set forth herein.

65. As alleged above, Defendants violated BIPA by failing to develop a written policy that it made available to the public that established a retention schedule and guidelines for permanently destroying biometric identifiers and information.

66. Defendants' violations of BIPA were intentional and reckless or, pleaded in the alternative, negligent.

67. As a direct and proximate result of Defendants' violations of BIPA, Plaintiffs and Class Members have suffered and will continue to suffer injury.

68. Plaintiffs and Class Members seek as monetary relief the greater of $5,000 or actual damages or, pleaded in the alternative, $1,000 or actual damages.

69. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for their injuries in that a judgment for monetary damages will not end the misuse of Plaintiffs' and Class Members' biometric identifiers and information.

70. Plaintiff and Class Members also seek punitive damages, injunctive relief and the reasonable attorney's fees, costs and expenses relating to this action.

COUNT TWO
(VIOLATION OF BIPA – 740 ILCS § 14/15(b))

71. Plaintiffs restate and reallege all paragraphs of this Class Action Complaint as though fully set forth herein.

72. As alleged above, Defendants violated BIPA by collecting, capturing, and otherwise obtaining individuals' biometric identifiers and information, including the biometric identifiers and information of Plaintiffs and Class Members, without providing the requisite written information and without obtaining the requisite written releases.

73. Defendants' violations of BIPA were intentional and reckless or, pleaded in the alternative, negligent.

74. As a direct and proximate result of Defendants' violations of BIPA, Plaintiffs and Class Members have suffered and will continue to suffer injury.

75. Plaintiffs and Class Members seek as monetary relief the greater of $5,000 or actual damages or, pleaded in the alternative, $1,000 or actual damages.

76. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for their injuries in that a judgment for monetary damages will not end the misuse of Plaintiffs' and Class Members' biometric identifiers and information.

77. Plaintiffs and Class Members also seek punitive damages, injunctive relief and the reasonable attorney's fees, costs and expenses relating to this action.

COUNT THREE

(VIOLATION OF BIPA – 740 ILCS § 14/15(c))

78. Plaintiffs restate and reallege all paragraphs of this First Amended Class Action Complaint, as though fully set forth herein.

79. As alleged above, Defendants violated BIPA by selling, leasing, trading, and unlawfully profiting from individuals' biometric identifier or biometric information, including the biometric identifiers and information of Plaintiffs and Class Members.

80. Defendants' violations of BIPA were intentional and reckless or, pleaded in the alternative, negligent.

81. As a direct and proximate result of Defendants' violations of BIPA, Plaintiffs and Class Members have suffered and will continue to suffer injury.

82. Plaintiffs and Class Members seek as monetary relief the greater of $5,000 or actual damages or, pleaded in the alternative, $1,000 or actual damages.

83. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for their injuries in that a judgment for monetary damages will not end the misuse of Plaintiffs' and Class Members' biometric identifiers and information.

84. Plaintiffs and Class Members also seek punitive damages, injunctive relief and the reasonable attorney's fees, costs and expenses relating to this action.

COUNT FOUR
(VIOLATION OF BIPA – 740 ILCS § 14/15(d))

85. Plaintiffs restate and reallege all paragraphs of this Class Action Complaint as though fully set forth herein.

86. As alleged above, Defendants violated BIPA by disclosing, redisclosing and otherwise disseminating individuals' biometric identifiers and information, including the biometric identifiers and information of Plaintiffs and Class Members, even though: (a) neither the subjects of the biometric identifiers and information nor their authorized representatives consented to the disclosure and redisclosure; (b) the disclosure and redisclosure did not complete a financial transaction requested or authorized by the subjects of the biometric identifiers and information or their authorized representatives; (c) the disclosure and redisclosure was not required by State or federal law or municipal ordinance; and (d) the disclosure and redisclosure was not required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

87. Defendants' violations of BIPA were intentional and reckless or, pleaded in the alternative, negligent.

88. As a direct and proximate result of Defendants' violations of BIPA, Plaintiffs and Class Members have suffered and will continue to suffer injury.

89. Plaintiffs and Class Members seek as monetary relief the greater of $5,000 or actual damages or, pleaded in the alternative, $1,000 or actual damages.

90. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for their

injuries in that a judgment for monetary damages will not end the misuse of Plaintiffs' and Class Members' biometric identifiers and information.

91. Plaintiffs and Class Members also seek punitive damages, injunctive relief and the reasonable attorneys' fees, costs and expenses relating to this action.

COUNT FIVE
(VIOLATION OF BIPA – 740 ILCS § 14/15(e))

92. Plaintiffs restate and reallege all paragraphs of this Class Action Complaint as though fully set forth herein.

93. Defendants, while in possession of Plaintiffs' and Class Members' biometric identifiers and information, failed to protect from disclosure all biometric identifiers and information: (a) using the reasonable standard of care within its industry; and (b) in a manner that is the same as or more protective than the manner in which they protect other confidential and sensitive information.

94. Defendants' violations of BIPA were intentional and reckless or, pleaded in the alternative, negligent.

95. As a direct and proximate result of Defendants' violations of BIPA, Plaintiffs and Class Members have suffered and will continue to suffer injury.

96. Plaintiffs and Class Members seek as monetary relief the greater of $5,000 or actual damages or, pleaded in the alternative, $1,000 or actual damages.

97. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for their

injuries in that a judgment for monetary damages will not end the misuse of Plaintiffs' and Class Members' biometric identifiers and information.

98. Plaintiffs and Class Members also seek punitive damages, injunctive relief and the reasonable attorney's fees, costs and expenses relating to this action.

COUNT SIX
(UNJUST ENRICHMENT)

99. Plaintiffs restate and reallege all paragraphs of this Class Action Complaint as though fully set forth herein.

100. Defendants obtained a monetary benefit from Plaintiffs and Class Members to their detriment. Defendants did so by profiting off of the surreptitious collection of the biometric identifiers and information of Plaintiffs and Class Members, while exposing Plaintiffs and Class Members to a heightened risk of privacy harms and depriving them of their control over their biometric data.

101. Plaintiffs and Class Members did not authorize Defendants to collect, capture, obtain, disclose, redisclose, disseminate, sell, trade, lease, and otherwise profit off of their biometric identifiers and information.

102. Defendants appreciated, accepted and retained the benefit bestowed upon it under inequitable and unjust circumstances arising from Defendants' conduct toward Plaintiffs and Class Members as described herein.

103. Defendants sold, leased, traded and otherwise profited from – and caused to be sold, leased, traded and otherwise profited from – Plaintiffs' and Class Members' biometric identifiers and information and did not provide full compensation for the benefit received from Plaintiffs and Class Members.

104. Defendants acquired and caused to be acquired Plaintiffs' and Class Members' biometric identifiers and information through inequitable means in that it collected, captured and otherwise obtained biometric identifiers and information from Plaintiffs' and Class Members' online photos without permission and in violation of Illinois law.

105. Plaintiffs and Class Members have no adequate remedy at law.

106. Under the circumstances, it would be unjust and unfair for Defendants to be permitted to retain any of the benefits obtained from Plaintiffs and Class Members and their biometric identifiers and information.

107. Under the principles of equity and good conscience, Defendants should not be permitted to retain the biometric identifiers and information belonging to Plaintiffs and Class Members because Defendant unlawfully obtained that information.

108. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received as a result of its collection, capture, obtainment, disclosure, redisclosure, dissemination, sale, leasing, trading, and profiting off of Plaintiffs' and Class Members' biometric identifiers and information.

COUNT SIX
INJUNCTIVE RELIEF

109. Plaintiffs restate and reallege all paragraphs of this Class Action Complaint as though fully set forth herein.

110. Plaintiffs and Class Members have clear and ascertainable rights in need of protection – namely: (a) the right to have Defendants abide by its obligations under BIPA; (b) the right to control their biometric identifiers and information; and (c) the right to privacy.

111. Plaintiffs and Class Members have no adequate remedy at law because a legal remedy cannot retrieve the biometric identifiers and information that Defendants unlawfully collected, captured, obtained, disclosed, redisclosed, disseminated, sold, leased, traded, and otherwise profited from, and cannot end the invasion of privacy caused by Defendants' conduct.

112. Plaintiffs and Class Members will suffer irreparable harm, as alleged herein, from Defendants if its conduct is not so restrained, requiring injunctive relief.

113. Plaintiffs and Class Members are likely to succeed on the merits because, as alleged herein, Defendants unlawfully collected, captured, obtained, disclosed, redisclosed, disseminated, sold, leased, traded, and otherwise profited from Plaintiffs' and Class Members' biometric identifiers and information despite being prohibited from doing so.

114. Plaintiffs and Class Members seek injunctive relief: (a) barring Defendants from any further use of Plaintiffs' and Class Members' biometric identifiers and information; (b) barring Defendants from continuing to collect, capture, obtain, disclose, redisclose, disseminate or profit from Plaintiffs' and Class Members' biometric identifiers and information; and (c) requiring Defendants to delete and destroy Plaintiffs' and Class Members' biometric identifiers and information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and on behalf of the Class, respectfully seek from the Court the following relief:

a. Certification of the Class as requested herein;

b. Appointment of Plaintiffs as Class representatives and their undersigned counsel as Class counsel;

c. An award of damages for Plaintiffs and members of the proposed Class, including statutory and punitive damages;

d. An order requiring deletion of the biometric identifiers and information of Plaintiffs and members of the proposed Class;

e. An award of equitable, injunctive and declaratory relief for Plaintiffs and members of the proposed Class, including an injunction (i) barring Defendants from any further use of individuals' biometric identifiers and information; (ii) barring Defendants from continuing to collect, capture, obtain, disclose, redisclose, disseminate and profit from Plaintiffs' and Class Members' biometric identifiers and information; (iii) requiring Defendants to delete and destroy all biometric identifiers and information in its possession, custody and control; and (iv) requiring Defendants to claw back the biometric identifiers and information from any third parties to whom they disclosed, redisclosed and disseminated it;

f. An order requiring Defendants to disgorge into a common fund or constructive fund, for the benefit of Plaintiffs and members of the proposed Class, proceeds that it unjustly received as a result of its collection, capture, obtainment, disclosure, redisclosure, dissemination and profiting off of the biometric identifiers and information of Plaintiffs and members of the proposed Class;

g. An award of pre-judgment and post-judgment interest for Plaintiffs and members of the proposed Class, as permitted by law

h. An award for Plaintiffs and members of the proposed Class of reasonable attorneys' fees and costs of suit, including expert witness fees; and

i. An award for Plaintiffs and members of the proposed Class of any further relief the Court deems proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial on all claims so triable.

Dated: February 14, 2020

Respectfully submitted,

/s/ Mike Kanovitz
MICHAEL KANOVITZ

Arthur Loevy
Michael Kanovitz
Jon Loevy
Scott R. Drury
LOEVY & LOEVY
311 N. Aberdeen, 3rd Floor
Chicago, Illinois 60607
312.243.5900
arthur@loevy.com
mike@loevy.com
jon@loevy.com
drury@loevy.com